# CASO 2009 M57-JEAN

PRESENTADO POR:

YENI VIVIANA PATIÑO MENDIGAÑO

JHON JAIRO RODRIGUEZ CABEZAS

UNIVERSIDAD PILOTO DE COLOMBIA

SECCIONAL ALTO MAGDALENA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

INFORMATICA FORENSE

GIRARDOT

2022

# CASO 2009 M57-JEAN

PRESENTADO POR:

YENI VIVIANA PATIÑO MENDIGAÑO

21710343

JHON JAIRO RODRIGUEZ CABEZAS

21710289

EDICSON PINEDA CADENA

DIRECTOR MONOGRAFIA

UNIVERSIDAD PILOTO DE COLOMBIA

SECCIONAL ALTO MAGDALENA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

INFORMATICA FORENSE

GIRARDOT

2022

Agradecimientos a Dios y a cada uno de nuestros seres queridos quienes nos han guiado en este camino, brindándonos el apoyo incondicional.

## Índice de Contenido

## Índice de Tablas



## Índice de ilustraciones

## RESUMEN

El objetivo primordial de esta investigación, es analizar la copia forense byte a byte que se generó de la computadora portátil del director financiero Jean de la empresa M57 dotbiz y así determinar de qué manera se presentó la filtración de datos.

En el caso M57 Jean (2009), busca dar a conocer un problema de fuga de datos empresariales, lo que se clasifica como "Alta Confidencialidad". Los hechos suceden a partir de una filtración de un documento tipo hoja de cálculo de Excel, encontrada en la computadora del ya mencionado director financiero. Cabe aclarar que dicha información no debería ser suministrada a ningún funcionario de la empresa, ya que esta contenía información personal de sus empleados, como lo son sus nombres, apellidos, salario y números de identificación personal. Todo esto se logra evidenciar a través de un análisis forense realizado a la imagen Encase.

Para el desarrollo de la investigación, se usó el software forense "Autopsy" el cual nos suministró un informe detallado de los sucesos que se llevaron a cabo en la computadora; también se encontraron unos mensajes enviados a través de la plataforma de Microsoft Outlook 2000, donde se observan unas conversaciones entre la presidente y el director financiero; en donde le solicita generar dicha hoja de cálculo.



**Palabras claves:** Análisis Forense, Autopsy, Hoja de Cálculo, Computadora, Encase, Microsoft Outlook.

## ABSTRACT

The main objective of this investigation is to analyze the byte-by-byte forensic copy that was generated from the laptop of the financial director Jean of the company M57 dotbiz and thus determine how the data leak occurred.

In the case of M57 Jean (2009), it seeks to publicize a business data leak problem, which is classified as "High Confidentiality". The events take place from a leak of an Excel spreadsheet type document, found on the computer of the aforementioned financial director. It should be clarified that said information should not be provided to any company official, since it contained personal information of its employees, such as their names, surnames, salary and personal identification numbers. All this is evidenced through a forensic analysis carried out on the Encase image.

For the development of the investigation, the forensic software "Autopsy" was used, which provided us with a detailed report of the events that took place on the computer; messages sent through the Microsoft Outlook 2000 platform were also found, where conversations between the president and the financial director are observed; where she asks you to generate said spreadsheet.



Keywords: Forensic Analysis, Autopsy, Spreadsheet, Computer, Encase, Microsoft Outlook.

# INTRODUCCIÓN

Hoy por hoy la informática forense ha sido una herramienta clave para la solución de problemas graves enfocados a delitos informáticos, ya que esta busca entender cómo sucedieron los hechos y así mismo poder brindar un veredicto de la realidad de lo ocurrido.

Según el autor Lázaro define la informática forense como " el empleo de métodos científicos comparables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidencias digitales precedentes a fuentes digitales con el propósito de hacer posible la reconstrucción de hechos considerados delictivos o ayudar a la prevención de actos no autorizados capaces de provocar una alteración en operaciones planificadas de organismos y empresas" (Lázaro Domínguez, 2014) y para ello es necesario la ejecución de los siguientes pasos la adquisición, el análisis, la presentación y una línea de tiempo, los cuales nos permitirán esclarecer que fue lo que sucedió para así mismo obtener las pruebas o datos que prueben si se ha realizado o no algún delito informático para así mismo entregar unos resultados ya sea, ante una corte, o ante una junta directiva, etc.

En este caso, orientado a este documento, lo que se quiere llegar a demostrar y comprobar es ¿Qué sucedió? Con la filtración de información confidencial del ca, así mismo dando a conocer el paso a paso que se realizó para llegar a la conclusión junto con toda la información que se pueda llegar a recolectar de la misma, para ello se utilizará la herramienta autospy la cual nos permitirá analizar información tales como imágenes y códigos abiertos que fueron borrados y modificados.

# OBJETIVOS

## Objetivo General

Realizar un análisis forense detallado al CASO 2009 M57-JEAN, en donde se pueda llegar a esclarecer la realidad de los hechos.

## Objetivos Específicos

- Evaluar las pruebas existentes en el Caso M57 haciendo uso de las herramientas de la informática forense.

- Encontrar las pruebas suficientes para demostrar quién es el culpable en el caso.

- Aplicar la herramienta autopsy para evaluar información suministrada.

## MARCO TEÓRICO

Enfocado a la resolución de problemas con respecto a la investigación forense, según el libro introducción a la informática forense, “explica que para poder obtener resultados con la investigación, es necesario realizar una serie de pasos los cuales están enfocados a evitar que la prueba encontrada se altere, para así mismo poder obtener un resultado probatorio y a su vez obtener resultado clave para la investigación”. (Lázaro Domínguez, 2014)

En la actualidad encontramos en nuestro territorio colombiano la aplicación de las tecnologías forenses, dejando huella positiva al momento de esclarecer los hechos en los sectores de entidades financieras, aportando de manera significativa “las herramientas informáticas usadas en una auditoría forense en las cooperativas de ahorro y crédito del sector financiero de la ciudad de Ibagué, Colombia, partiendo de identificar las herramientas utilizadas en una auditoria forense, y de establecer la percepción de los funcionarios de entidades cooperativas acerca de los fraudes en las cooperativas de ahorro y crédito del sector financiero, y luego proponer a partir del empleo de estas herramientas informáticas, soluciones para la prevención de delitos contra el orden económico social. En el desarrollo del manuscrito se utilizó el método deductivo, puesto que el proyecto parte de situaciones generales que llegan a explicar situaciones particulares contenidas explícitamente en la situación general. Si bien se presume que las herramientas informáticas en la era digital son aliadas fundamentales en el control organizacional, en las entidades consultadas se observan bajos niveles de

apropiación tecnológica en el área de control y aseguramiento del riesgo, lo que evidencia fisuras en la actualización tecnológica, la dimensión de desarrollo organizacional de los directivos y en la construcción del ideario regional sobre los peligros a los que se exponen las entidades que tienen carencias tecnológicas". **(Adolfo Rubio-Rodríguez, 2021)**.

**Prueba Pericial:** Son profesiones expertos en el análisis y recuperación de pruebas informáticas; en el que se realiza un exhaustivo recorrido de los hechos en los cuales se encuentran informes o archivos que puedan llegar a esclarecer o cambiar el rumbo de los hechos; no obstante permite tener un veredicto más acertado de las pruebas recolectadas.

**MD5 y SHA:** Son programas de cifrado que a partir de un mensaje de tamaño variable que está compuesto por un número determinado de caracteres alfanuméricos (código binario o cualquier otro tipo de carácter) calculan una secuencia de caracteres de longitud fija. (Lázaro Domínguez, 2014)

**dcfldd, dc3dd y ddrescue:** Estos tres programas están basados en el sistema de comandos DD, el cual su código fuente es libre y hasta el momento todo aquel persona puede adaptarlo para que incorpore nuevas características. El programa dcfldd extrae y valida hashes de forma paralela, significa que lleva un registro de la actividad y posteriormente divide la imagen en fragmentos de tamaño fijo que llegan a facilitar su almacenamiento y manipulación de la información. Por otra parte, el programa dc3dd que fue desarrollado por Jesse Komblum, es un parche el cual incorpora nuevas características de dd con mayor rapidez que dcfldd. Y con ddrescue nos menciona que, si un soporte de datos

posee sectores defectuosos, estos los podemos llegar a adquirir a través de dd especificando la opción conv=noerror,sync. Cuando se hace este proceso las partes ilegibles serán reemplazadas por ceros. (Lázaro Domínguez, 2014)

**AIR (Automated image and restore):** Es un front end para dd y dc3dd, que permite manejar de manera fácil y sencilla las opciones habituales, utilidades en línea de comando del apartado mencionado anteriormente. A la hora de realizar la imagen forense, esta interfaz verifica la copia de los hashes MD5 o SHA 1/256/384/512, comprime y descomprime la imagen mediante un archivo gzip/bzip2, ofreciendo la posibilidad de transferirla a un host remoto a través de redes de TCP/IP. (Lázaro Domínguez, 2014)

## MARCO LEGAL

Dentro de la normativa colombiana vigente enfocada al caso Jean 2019 M57 se encuentran las siguientes leyes y decretos, por los cuales dicha persona que filtro la información puede ser acusada.

Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”

Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.”

Decreto 1727 de 15 de mayo de 2009 “por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia,

comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información."

Ley 1918 del 24 de julio del 2018 "por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest."

**MARCO CONTEXTUAL**

Se evidencia en el caso de la empresa M57 ocurrido en el año 2008, en la que dicha empresa ha sufrido un posible ataque cibernético, en donde fue manipulada la información de los colaboradores; el principal temor es que la información robada sea divulgada a la competencia y de este modo se pueda llegar a perder a sus colaboradores; de igual manera la presidente Alison en compañía de Jean buscan esclarecer la realidad de los hechos lo que deja como evidencia clave correos electrónicos y una laptop.

El principal interés es el esclarecimiento del caso M57 es poder evaluar los posibles ataques informáticos que se pueden llegar a encontrar y de esta manera entender de qué modo poder resolverlos.

**MARCO CONCEPTUAL:**

**CarvedFiles o Tallado de Archivos:**

El tallado de archivos o file carving es una técnica que usa en la informática forense con la finalidad de la extracción de unos archivos o datos que fueron formateados de una unidad de disco duro de almacenamiento, sin la utilización del sistema de archivos que se creó originalmente en la copia forense. Es usada para

recuperar ficheros en la zona no reservada del disco duro, significa que esta área del disco no hay nada almacenado desde el punto de visa de la estructura del sistema de archivos. (Sánchez, 2010)

**OrphanFiles O Archivos huérfanos:**

Es un archivo en una computadora que se vuelve obsoleto en el momento en que en la aplicación lo ha movido o eliminado de su sistema. Una de las razones principales cuando un archivo se vuelve huérfano, es cuando en el sistema operativo se presenta una desinstalación incompleta de algún software o programa. Por ejemplo, cuando en el sistema operativo Windows en vez de eliminar el programa directamente desde el panel de control, eliminamos solamente el acceso directo al programa, ya en ese proceso se generan archivos huérfanos.

**Imagen Forense:**

Una imagen forense es una copia bit a bit exacta de un dispositivo de almacenamiento sea disco duro, memoria USB, disco CD o DVD y disquete. Es también conocido como una imagen de flujos de bits. En otras palabras, cada bit (1 o 0) es duplicado en otro dispositivo limpio desde la perspectiva forense, como un disco duro. (Quezada, 2018)

**Encase:**

Es un formato de imagen forense el cual almacena evidencia digital incluyendo imágenes de volúmenes o particiones de un disco duro. Este formato Encase crea varias imágenes empezando con la extensión E01. Una de las características más distintiva de este formato de imagen forense, es que cambia la

extensión del archivo para cada nuevo archivo que se cree en la imagen analizada, por ejemplo, E01, E02, E03, E04 hasta E∞.

**dd:**

Es un comando incluido en sistemas operativos tipo Unix, consiste en recolectar partes de un archivo y después copiarlos a otro, con este comando podemos obtener una copia tipo RAW (copia en bruto o crudo) del soporte de datos, el cual después podemos someter a operaciones de hash y de analizar cualquier software de investigación forense. (Lázaro Domínguez, 2014)

**Perito Forense:**

Es una labor de análisis llevada a cabo por cualquier experto que es llamado a intervenir como perito en un proceso judicial, el cual asume un papel de tercero, ajeno al litigio. Debe tener la capacidad de comunicar sus hallazgos a un tribunal de forma clara.

**Pst:**

La extensión .pst, es un archivo de datos de Microsoft Outlook que almacena mensajes y otros elementos de manera remota en la computadora. En este caso la mayoría de los mensajes que mantuvo el director financiero Jean fue por medio de la plataforma de Microsoft Outlook 2000 a través de un archivo de nombre “outlook.pst”.

## MARCO METODOLOGICO

### Adquisición

En este paso es importante que toda la información que se tome sea por medio de una copia al disco original, es decir, que se realice una copia de seguridad de manera completa de toda la información que se almacene en el disco, Lázaro explica que dentro de la copia se debe incluir “el espacio no asignado por los sistemas de archivos, los archivos borrados e incluso datos que pudieran haber existido antes de que el soporte fuese formateado” (Dominguez Lázaro, 2014); para que esto se lleve a cabo, es necesario disponer de herramientas y/o aplicaciones que nos permitan realizar este tipo de toma de información, dentro de las aplicaciones que destaca el autor se encuentran dd, EnCase, FTK, Air, entre muchas más herramientas, las cuales serán capaces de obtener dichos resultados.

Para el escenario M57-Jean 2009 se tiene como evidencia desde la página web “Digital Corpora” una imagen forense del tipo Encase (E01) de la cual contiene toda la información del disco de almacenamiento de la computadora portátil del CFO de M57 dotbiz el cual es Jean.

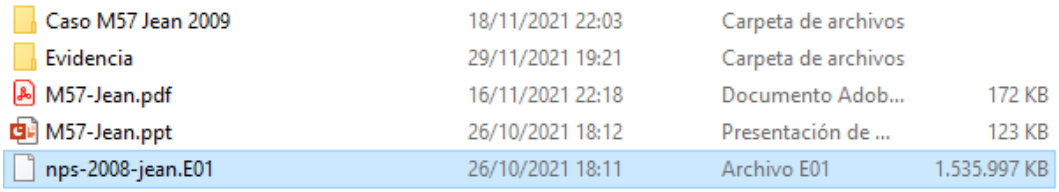


*Ilustración 1 Imagen Forense Encase Descargada para el análisis del Caso*

*Tabla 1 Especificaciones Imagen Encase (E01)*

| **Tabla No. 1 Especificaciones Imagen Encase (E01)** |
|---|

| En esta tabla se da a conocer las especificaciones técnicas que tiene la imagen forense tipo encase para este escenario de la empresa M57 dotbiz a través del software libre Autopsy 4.19.1. | | |
|---|---|---|
| **No.** | **Nombre** | **Descripción** |
| 1 | Nombre | nps-2008-jean.E01 |
| 2 | Tipo | Imagen Encase (.E01) |
| 3 | Tamaño (bytes) | 10737418240 |
| 4 | Tamaño del Sector | 512 Bytes |
| 5 | Cantidad Volúmenes | Volumen 1, 2 y 3. |
| 6 | MD5 | 78a52b5bac78f4e711607707ac0e3f93 |
| 7 | SHA1 | Not calculated |
| 8 | SHA-256 | Not calculated |
| 9 | Device ID | 12e99ae4-b15a-496b-94f5-4693edb95a1e |

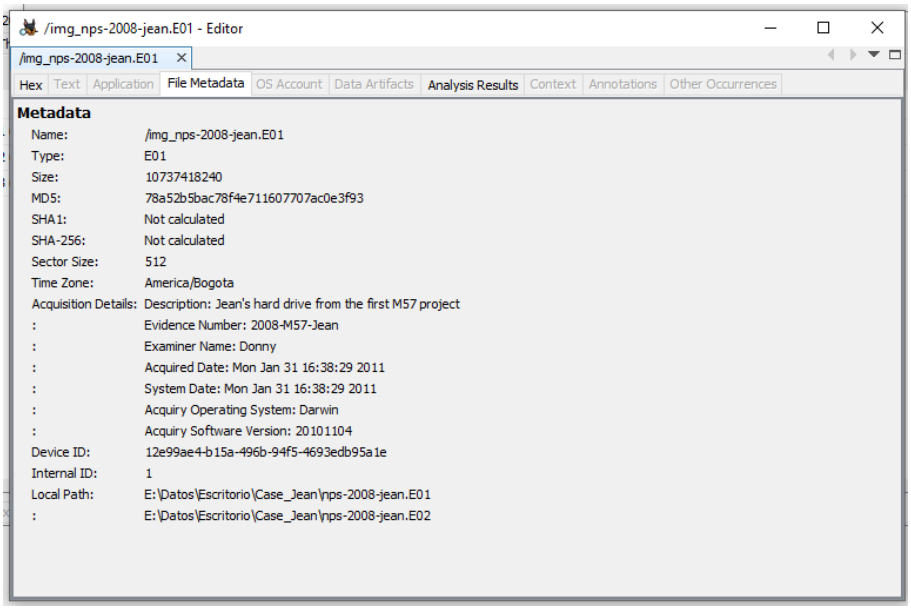


*Ilustración 2 Especificaciones Imagen Encase*

*Tabla 2 Especificaciones Volumen 2 de Imagen Encase*

| Tabla No.2 Especificaciones Volumen 2 de Imagen Encase | | |
|---|---|---|
| En la tabla No. 2 obtener con mayor informaciones las especificaciones que se llegaron a encontrar en el análisis de la imagen forense Encase (E01) por medio del software libre Encase 4.19.1. | | |
| **No.** | **Nombre** | **Descripción** |
| 1 | Nombre | vol2 (NTFS / exFAT (0x07): 63-20948759) |
| 2 | Sector de inicio | 63 |
| 3 | Longitud en sectores | 20948697 |
| 4 | Descripción | NTFS / exFAT (0x07) |
| 5 | Tipo de Sistema de Archivos | NTFS |
| 6 | Desplazamiento de imagen | 32256 |
| 7 | Tamaño de bloque | 4096 Bytes |

| | | |
|---|---|---|
| 8 | Recuento de bloques | 2618587 |
| 9 | Última entrada de metadatos | 32848 |

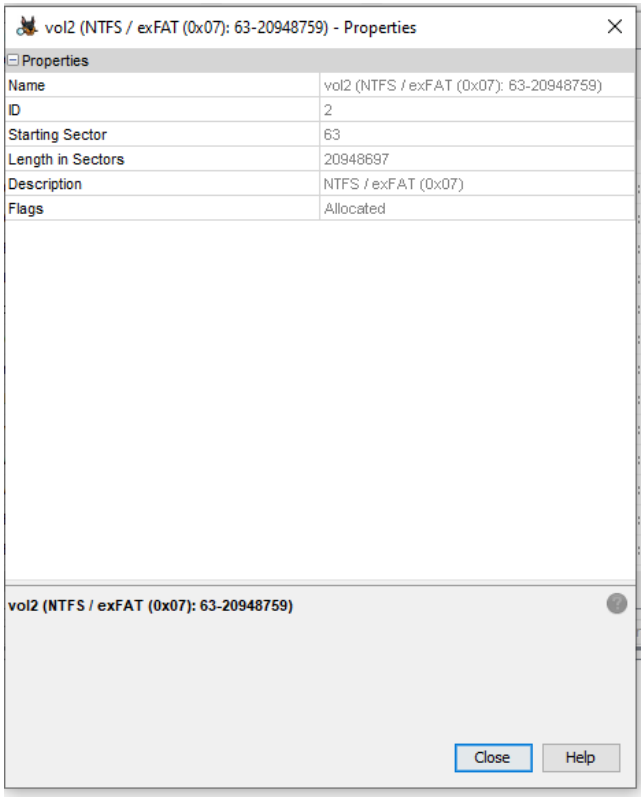


*Ilustración 3 Propiedades Volumen 2*

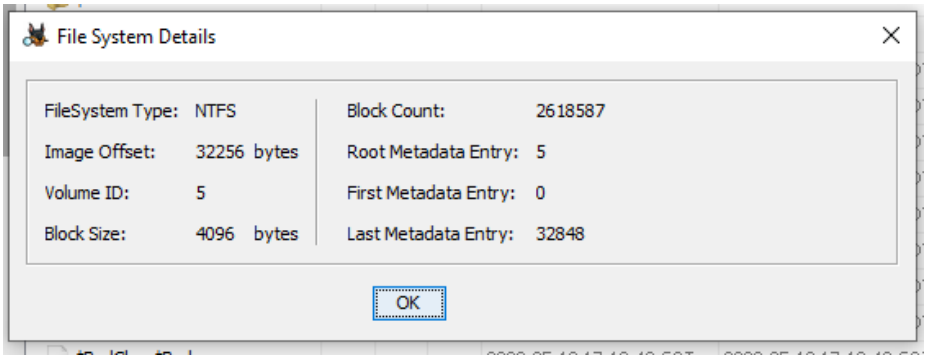


*Ilustración 4 Detalles Sistema de Archivos Volumen 2*

## Análisis

Según Lázaro "El análisis consiste en la identificación, el estudio y la interpretación de los elementos de evidencia existentes en el soporte de datos"

(Domínguez, 2014) Dentro de este paso, es importante que el investigador forense evalué cada uno de los datos obtenidos, para que así mismo determine que archivos se consideran sospechosos y conozca detalladamente el contenido de los mismos; y así mismo cuando evalué y analice cada uno de los archivos este, puede dar una conclusión o un veredicto de lo que sucedió.

Resumen de entrevistas a las dos personas involucradas en este caso M57.

**Alison (Presidenta)**

- No sé de qué está hablando Jean.
- Nunca le pedí a Jean la hoja de cálculo.
- Nunca recibí la hoja de cálculo por correo electrónico.

**Jean (director financiero)**

- Alison me pidió que preparara la hoja de cálculo como parte de la nueva ronda de financiación.
- Alison me pidió que le enviara la hoja de cálculo por correo electrónico.
- Eso es todo lo que sé.

**Evidencia encontrada en la imagen forense tipo Encase (E01)**

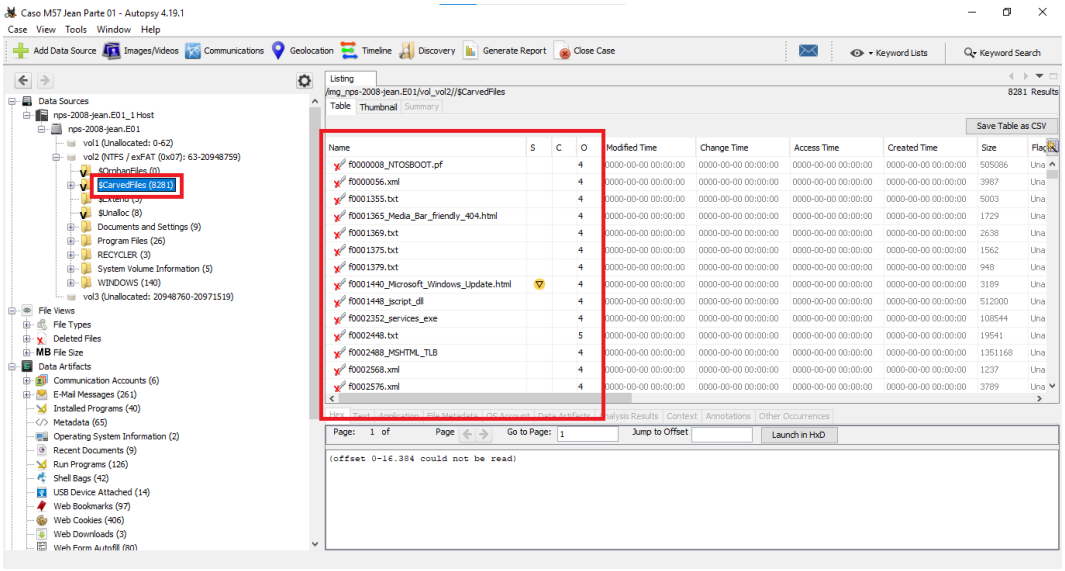


*Ilustración 5 Total de Archivos Tallados en la imagen Encase E01*

En el volumen 2 de la imagen forense de nombre “nps-2008-jean.E01” se halla un total de 8281 archivos tallados que fueron borrados del sistema de archivos del disco de almacenamiento de la computadora portátil del CFO Jean.

En esta imagen forense respecto al disco de almacenamiento de la computadora portátil de Jean de la empresa M57 dotbiz, se encuentran los siguientes volúmenes:

| Name | ID | Starting Sector | Length in Sectors | Description | Flags |
|---|---|---|---|---|---|
| vol1 (Unallocated: 0-62) | 1 | 0 | 63 | Unallocated | Unallocated |
| vol2 (NTFS / exFAT (0x07): 63-20948759) | 2 | 63 | 20948697 | NTFS / exFAT (0x07) | Allocated |
| vol3 (Unallocated: 20948760-20971519) | 3 | 20948760 | 22760 | Unallocated | Unallocated |

*Ilustración 6 Volúmenes encontrados en la primer imagen E01*

Como se logra observar en la ilustración no. 5 se encuentran 8281 archivos tallados que fueron formateados del disco duro de la computadora de Jean, pero solamente en la siguiente ruta “vol2/Documentos and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst” se encuentra un archivo Outlook.pst el cual contiene conversaciones que mantuvo el director financiero Jean

con la presidenta Alison y otros compañeros de la empresa mencionada en este caso, a través de la plataforma de Microsoft Outlook 2000.

Mensajes a través de la plataforma Microsoft Outlook 2000 entre el director Financiero Jean y la presidenta Alison de la empresa M57 dotbiz.

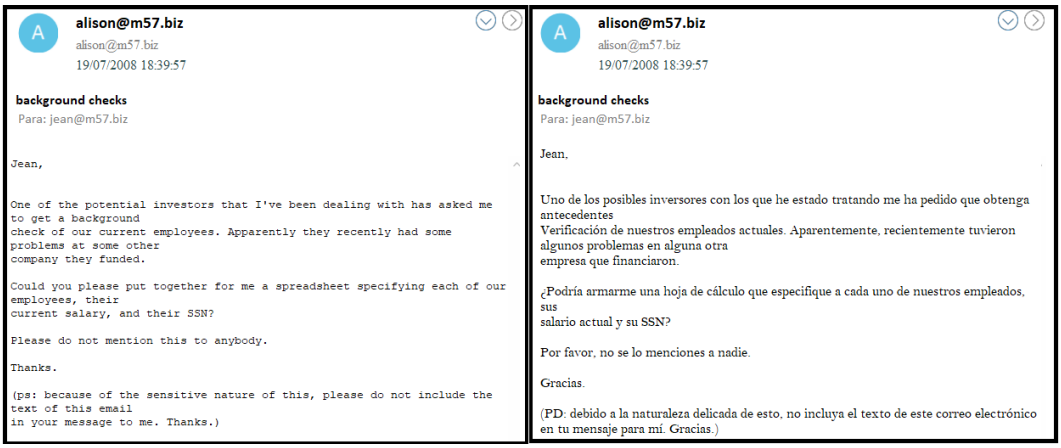


*Ilustración 7 Primer Evidencia mensaje de Alison a Jean*

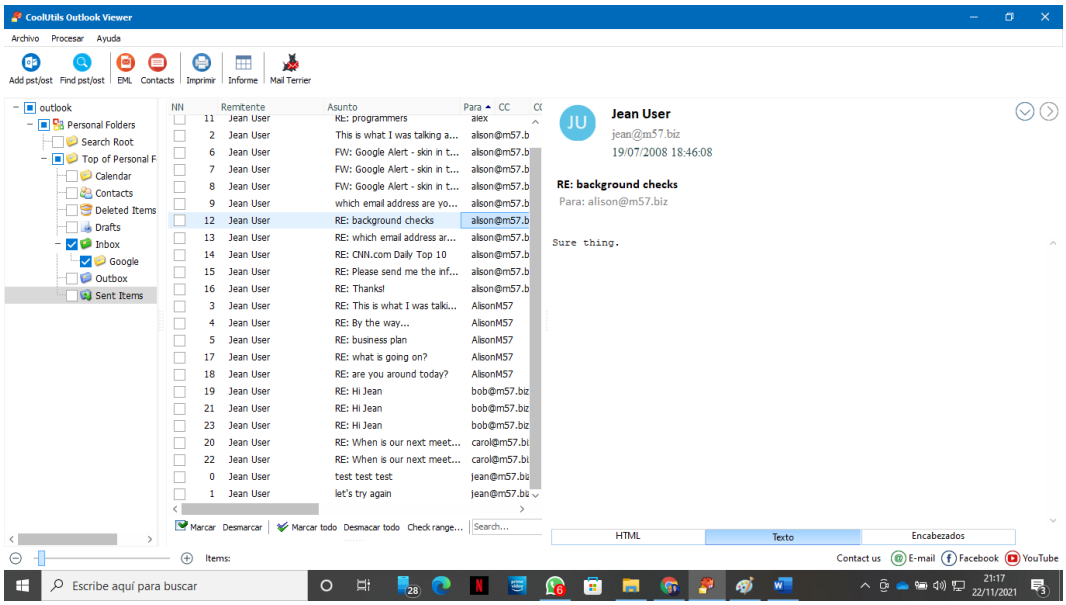


*Ilustración 8 Segunda Evidencia Respuesta de Jean a Alison del mensaje de "background checks"*

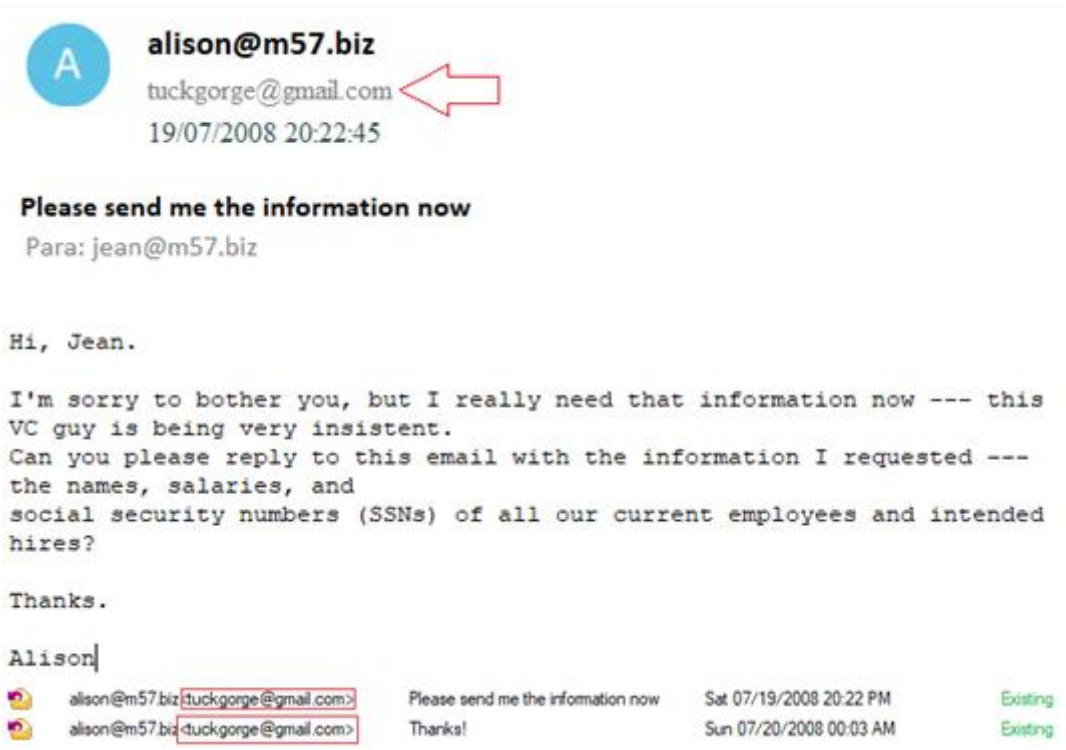


*Ilustración 9 Tercera Evidencia Mensaje de Alison a Jean del mensaje "Por favor envíame la información ahora"*

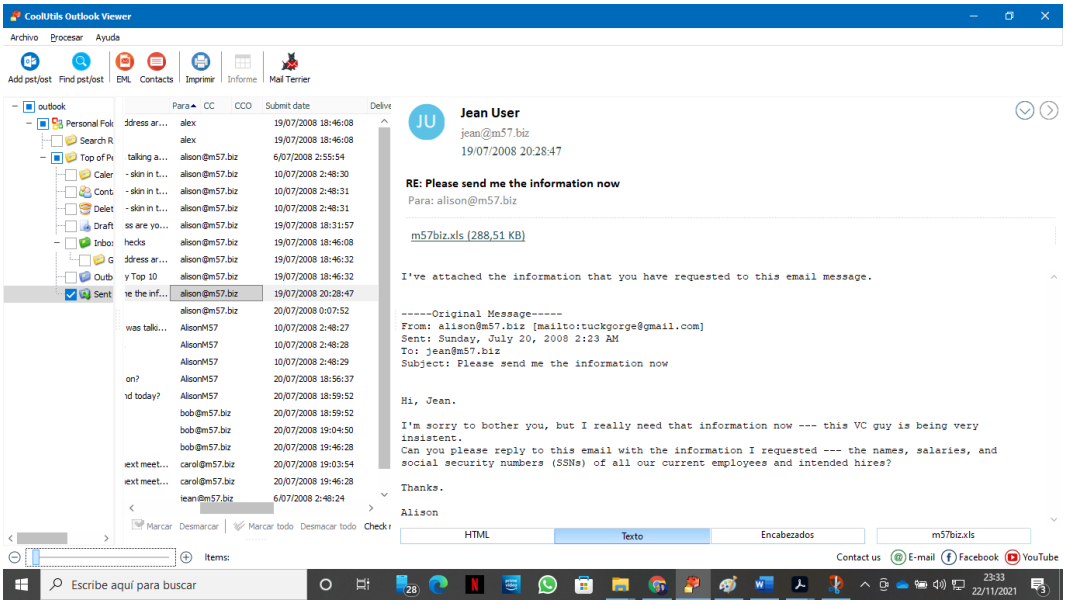


*Ilustración 10 Cuarta Evidencia Envió Hoja de Cálculo Información Empleados al Correo electrónico "tuckgorge@gmail.com" Infiltrado*

**Presentación**

En este paso, el investigador forense recopila toda la información encontrada y la transforma en un informe de fácil entendimiento para alguien que no es conocedor de informática, por otro lado, es importante que el investigador deje en constancia todos los pasos que realizó, toda la información que recopiló, para que así mismo esta información sea utilizada como prueba ante un caso en concreto.

En el volumen 2 de la imagen forense de nombre “nps-2008-jean.E01” se halla un total de 8281 archivos tallados que fueron borrados del sistema de archivos del disco de almacenamiento de la computadora portátil del CFO Jean.

Entre los archivos borrados se encuentran imágenes en formato jpg, png, gif. Archivos tipo de acceso directo y de aplicaciones. Documento de texto tipo Word, txt, hojas de cálculo xls y archivos dll.

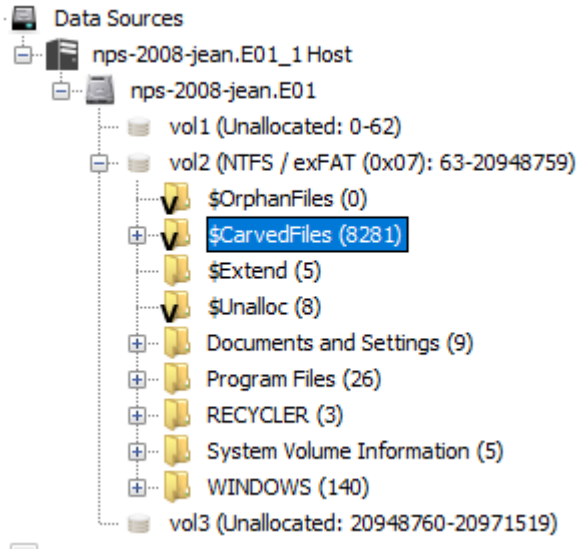


*Ilustración 11 Archivos Tallados Imagen Forense*

En la ilustración no. 7 con el asunto de “verificaciones de antecedentes o background checks” la presidenta Alison le está pidiendo a Jean que arme una hoja de cálculo en donde especifique a cada uno de los empleados de M57 dotbiz, su salario actual y sus ssn, ya que uno de los posibles inversores que han tratado con Alison le está pidiendo antecedentes de la empresa, la verificación de los empleados actuales de la empresa. Y de igual manera le pide a Jean que no se lo mencione a nadie y que ni tampoco en el asunto del mensaje incluya el texto de este correo electrónico. En pocas palabras que sea lo más discreto posible con la información que le está solicitando Alison.

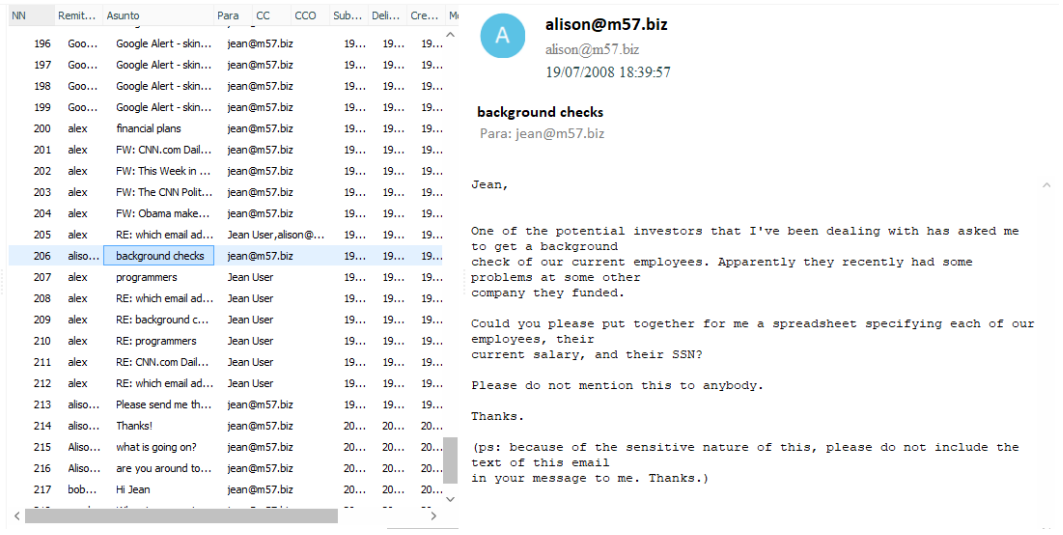


*Ilustración 12 Mensaje "Background Checks" de Alison*

En la ilustración no. 8 le responde Jean a la presidenta Alison, si está segura en cuanto a que le envíe esa información delicada de la empresa M57 dotbiz.

En la ilustración no. 9 se logra visualizar un cambio significativo en el mensaje que recibió Jean el día 19 de julio de 2008 a las 20:22:45, debido a que el

correo del que fue enviado este mensaje, pasa de ser un correo corporativo de la empresa M57 a ser un correo personal, tal cual como se logra evidenciar en esta ilustración. Nos dice que este mensaje lo ha enviado una persona con el nombre de usuario del correo de la presidenta Alison el cual es “alison@m57.biz” a través del correo electrónico personal “tuckgorge@gmail.com” de la plataforma de Gmail.


*Ilustración 13 Visualizado del Encabezado del mensaje del correo personal infiltrado en la empresa a través del software “CoolUtils Outlook Viewer”*

**Línea de Tiempo**

Este paso es importante, ya que, por medio de herramientas informáticas, el investigador puede obtener una lista de los procesos que ocurrieron, la fecha en que ocurrieron y los cambios que se dieron allí; según Lázaro esto se utiliza para

“ayudar al investigador a comprender la evolución de los hechos y las relaciones de causa y efecto existentes en los mismos” (Dominguez Lázaro, 2014)

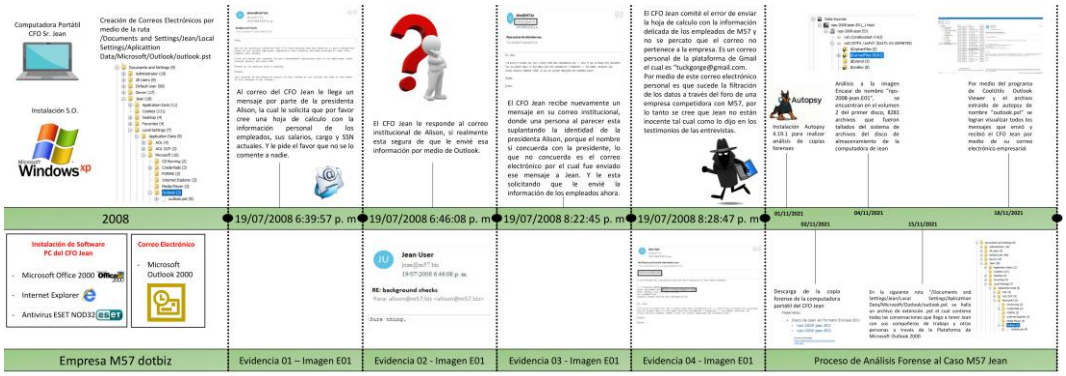


*Ilustración 14 Cronología gráfica del escenario M57 Jean*

## CONCLUSIONES

Se logra evidenciar manipulación ilegal de la información de la empresa y/o personal de los colaboradores.

Para poder llegar a esclarecer los hechos es importante el uso de las herramientas forenses ya que gracias a ello podemos determinar lo que realmente sucedió.

Manejo inadecuado de correo corporativo; los equipos no contaban con la correspondiente seguridad en cuanto sus contraseñas, lo que permite un alto grado de vulnerabilidad.

# MATERIAL COMPLEMENTARIO

## Referencias Bibliográficas


Domínguez, F. L. (2014). *Introducción a la Informática Forense.* España: RA-MA.

Lázaro Domínguez, F. (2014). *Introducción a la informatica forense.* Madrid: RA-MA.

Quezada, A. E. (04 de April de 2018). *reydes.com*. Recuperado el 14 de Noviembre de 2021, de http://www.reydes.com/d/?q=Imagenes_Forenses

Sánchez, A. (15 de Julio de 2010). *blog.elhacker.net*. Obtenido de https://blog.elhacker.net/2010/04/file-carving.html


## Bibliografía:


- https://www.whatisfileextension.com/es/e01/
- https://www.gp-grup.com/2019/05/peritaje-forense/
- https://es.calameo.com/read/005973800480afc089eaf?page=1
- https://forensis.cl/perito-conceptos-generales/
- https://eds.s.ebscohost.com/eds/detail/detail?vid=4&sid=9eb004fc-7b7c-4ff3-b28f-bdac2a28f456%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=edsbas.5D4A6A08&db=edsbas
-